Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 24 February 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The St. Louis Post−Dispatch reports Southern Commercial Bank may have compromised the privacy of thousands customers, and may have violated state and federal guidelines, by e−mailing unsecured personal data to an independent computer programmer. (See item 6)
- The Associated Press reports Amtrak officials will conduct a full investigation to determine how one of their passenger trains nearly collided with a freight train outside Syracuse, NY. (See item 11)
- Reuters reports the Department of Agriculture says a highly pathogenic strain of bird flu has been found in a Texas poultry flock −− this is a more serious type of the virus than that found in three other U.S. states. (See item 15)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *February 20, Las Vegas Review−Journal (NV)* — **Probe of tunnel notes ordered. Department of Energy (DOE) officials have initiated an investigation into whether Yucca Mountain Project field notes were altered to misrepresent tunnel workers' exposure to harmful silica dust.** The request is expected to form a base for a broader probe into worker health conditions during early excavation and peak tunneling at the nuclear waste repository

site a decade ago, DOE officials said Thursday, February 19. Margaret Chu, director of the Office of Civilian Radioactive Waste Management, called on DOE Inspector General Gregory Friedman to investigate how silica dust levels were recorded during construction of the Yucca Mountain exploratory tunnel. The program's present−day managers are trying to get their arms around the controversy, which reaches back years but came to light only in the past few months, Chu said. **Chu and Deputy Director John Arthur said they want a picture of worker conditions in the period between the initiation of mining activities, in 1992, and the 1995−96 period, when tunnel ventilation was improved and health protections were upgraded and enforced.** DOE has acknowledged officials were aware of potentially hazardous silica at Yucca Mountain, but workers were not given effective respiratory protections until 1996.
Source: http://www.reviewjournal.com/lvrj_home/2004/Feb−20−Fri−2004/news/23262669.html

2. *February 19, Tri−City Herald (WA)* — **Power supplies appear stable in Northwest. A winter that saw abundant snow in the lowlands still hasn't produced enough precipitation to rescue the Northwest out of what is looking like a fifth straight year of below− average runoff. Forecasts suggest there will be ample water to spin turbines at hydroelectric dams to meet power needs this year,** especially with electric demands suppressed by a lagging economy. In the long term, the region appears well equipped to meet energy needs in even below−average water years. The Northwest, which is consuming about 22,000 average megawatts, has about 1,000 megawatts to spare today and about zero chance of falling short at any point during the next several years, said John Fazio, a power systems analyst for the Northwest Power and Conservation Council.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5EZhjhlqmlUUfby30qbfej%5Bv

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *February 23, The Virginian−Pilot* — **Navy intranet is set to meet deadlines. It will take seven years and more than $8 billion to get the Navy Marine Corps Intranet (NMCI) up and running. The final product will connect more than 300,000 desktop computers to be shared by the Navy and Marines.** The largest federal information technology contract ever awarded, it represents one of the biggest cultural and technological changes the military has undertaken, and when it is finished, it could be the largest intranet in the world. The system is expected to be fully installed by the end of 2004 and will take another three years to become fully operational. The project is complicated because the Navy wanted to keep its existing systems running while the contractor built the new network. The prime contractor must consolidate 1,000 networks between the services −− at 300 bases around the world −− into a

single system. **The main desirable attribute, from the Department of Defense's standpoint, is that the system will be more secure than separate networks.**
Source: http://home.hamptonroads.com/stories/story.cfm?story=66464&r an=205121

4. *February 23, Associated Press* — **Navy begins aircraft carrier training off Florida Panhandle. Navy has begun its third aircraft carrier strike group exercise off the East Coast and in the Gulf of Mexico since ending live−fire training at Vieques Island in Puerto Rico four years ago. The carrier USS John F. Kennedy, four other surface ships and a submarine began the exercise Saturday, February 21, and will continue through mid−March.** The vessels are using Atlantic waters extending from Virginia to Florida and Eglin's gulf ranges off the Florida Panhandle. **The exercise is part of the Navy's Training Resource Strategy devised to use existing East Coast and Gulf Coast ranges and facilities and improved simulation technology to replace a bombing and gunnery range on Vieques.** Portions of the exercise, including naval gunfire, will be conducted against simulated land targets at sea. The current exercise includes the Kennedy and three other ships from Mayport Naval Station at Jacksonville, FL −− the guided missile cruiser USS Vicksburg, guided missile destroyer USS Roosevelt and destroyer USS Spruance. Also participating are the fast combat support ship USS Seattle from Earle, NJ, and the attack submarine USS Toledo from Groton, CT.
Source: http://www.heraldtribune.com/apps/pbcs.dll/article?AID=/2004 0223/APN/402230785

5. *February 17, United States Air Force* — **Transformation Flight Plan gives roadmap to future. Air Staff officials released the "Transformation Flight Plan," spelling out the future direction of the Air Force.** "Transformation is using new things and old things in new ways, and achieving truly transformational effects for the joint warfighter," said Lt. General Duncan McNabb, Air Force director of plans and programs. **In conjunction with joint partners, the Air Force is transforming by making capabilities−based changes in its operational concepts, organizational structures and/or technologies to expand the nation's military capabilities,** the general said. "The flight plan digs down into each of these areas in some detail, then links them all together to present a clear picture of where our Air Force is going in support of combatant commanders," General McNabb said. The flight plan will help Air Force people gain a perspective on the kind of skill sets and abilities they need to develop to help the service achieve its transformational goals. Transformation Flight Plan: http://www.oft.osd.mil/library/library_files/document_340_AF _TRANS_FLIGHT_PLAN_2003_FINAL_PUBLICLY_RELEASABLE_VERSION.pd f
Source: http://www.af.mil/mediacenter/pressrelease.asp?prID=12300700 2

[Return to top]

Banking and Finance Sector

6. *February 22, St. Louis Post−Dispatch (MO)* — **E−mail involves bank in privacy inquiry. Southern Commercial Bank, based in St. Louis, may have compromised the privacy of thousands customers, and may have violated state and federal guidelines, by e−mailing unsecured personal data to an independent computer programmer. The information included bank account and Social Security numbers as well as addresses for the customers, who have demand deposits and loans.** Southern Commercial officials said the

bank did not violate its own policies or federal regulations designed to protect customer information. The Missouri Division of Finance, which regulates Southern Commercial and other state−chartered banks, is investigating, said bank commissioner Eric McClure. Regulators are concerned because such information could be used to commit identity theft, either by the person who receives it or by someone who accesses the computer or the transmission. **The controversy involves computer programmer Rick Henderson, who said Tom Green, vice president at Southern Commercial's South Grand Boulevard branch, sent an e−mail in October that included personal bank account details in an attachment.** At the time, Henderson was a subcontractor, trying to finish work on a computer program that was to help the bank improve customer service. Henderson said he had received information on more than 40,000 of the bank's customers.
Source: http://www.stltoday.com/stltoday/business/stories.nsf/Business/9D53CE21E23D8AB486256E430024A17A?OpenDocument&Headline=E−mail+ensnarls+bank+in+privacy+inquiry

7. *February 21, Seattle Times (WA)* — **Police say arrest thwarts scam against truck maker. Police in Bellevue, WA, foiled a $214,000 scam against Paccar, the number three truck maker in the world,** and arrested a San Francisco, CA, woman on suspicion of theft and forgery. **The company was the victim of corporate−identity theft, said Bellevue police Officer Tory Mangione. He said the woman and up to three other unknown male accomplices obtained Paccar's accounting information and created phony paperwork, including purchase orders.** The woman and her accomplices apparently ordered 21 plasma−screen televisions over the Internet from a King County, WA, electronics store and then faxed the store a bogus purchase order, he said. The fraud was discovered when store employees contacted Paccar on February 13 to confirm the $214,000 purchase, he said.
Source: http://seattletimes.nwsource.com/html/eastsidenews/200186232 5_fraud21e.html

[Return to top]

Transportation Sector

8. *February 23, Associated Press* — **Mississippi River closed as crew search continues. Dozens of large ships and thousands of cruise passengers trying to get to or away from New Orleans as Mardi Gras fever builds up to a climax have been stranded while authorities mount a rescue mission.** The 178−foot Lee III sank on a foggy Saturday morning in the Southwest Pass, the only channel up the Mississippi River deep enough for large oceangoing vessels. The ship lay about 80 miles southeast of New Orleans, near where the river empties into the Gulf of Mexico. There was no way to tell when the river may reopen, said Coast Guard Petty Officer Jonathan McCool. **"It couldn't have happened on a worse weekend," said Gary LaGrange, chief of the Port of New Orleans. About 40 ships too big for alternate routes were waiting to enter Southwest Pass, and about the same number were waiting to leave port, said Lt. Rob Wyman, a Coast Guard spokesman.** Two large cruise ships scheduled to dock in New Orleans had to be diverted to east New Orleans and Gulfport, Miss. The cruise lines used buses to get thousands of passengers to and from temporary boarding points. The past few days have been a nightmare for river officials. Saturday's collision came just a day after the river had been reopened following a collision Thursday between a freighter and an oil tanker in which 22,000 gallons of oil were spilled.

Source: http://www.cnn.com/2004/US/South/02/22/ships.collide.ap/inde x.html

9. *February 23, KRT Wire* — **Security has improved at Charleston, WV, airport.** When Transportation Security Administration (TSA) employees operate Yeager Airport's baggage−screening machine, their eyes are searching for oddities. Cans of baked beans and jars of peanut butter sometimes set off the machine because they are similar in density to explosives. Certain shoe soles also can trip the alarm. Most of the time, the screeners determine that the 600 bags they screen daily in the airport's basement don't contain items prohibited on flights. TSA employees started screening passengers in August 2002, and they added baggage three months later. Lighter fluid is the most common hazardous material screeners find. **Screening has improved since the TSA took over at Yeager, said airport director Rick Atkinson. Before the TSA, the airlines paid Globe Security, a private company, to screen Yeager passengers. About 14 people worked for Globe at Yeager, compared to about 47 TSA−employed screeners.**
Source: http://www.miami.com/mld/miamiherald/business/national/80214 92.htm

10. *February 23, Manila Bulletin Online* — **Int'l airport security tightened; flaws noted. The Manila International Airport Authority has ordered its security forces to undergo re−training to enable the Ninoy Aquino International Airport (NAIA) to hurdle a 90−day reprieve issued by the U.S. Transportation Security Administration (TSA).** During its month−long audit that started last December, U.S. TSA officials found at least two major lapses in the implementation of security procedures at the country's premier airport. If the NAIA fails the security assessment, a public notice will be announced by the TSA worldwide, saying that it is not safe to travel in the Philippines. A similar remark will be stamped on airline tickets of all Manila−bound passengers. The review was scheduled to end last January, but was extended after U.S. TSA officials found some flaws in the implementation of NAIA's access control and baggage screening procedures, both considered vital tools against the global war on terrorism. These prompted TSA officials to place the NAIA on a three−month probation period to allow airport officials to correct the deficiencies and maintain levels of security procedures required by the International Civil Aviation Organization.
Source: http://www.mb.com.ph/MTNN200402243168.html

11. *February 23, Associated Press* — **Amtrak probes near collision with CSX freight train.** Amtrak officials will conduct a full investigation to determine how one of their passenger trains nearly collided Friday, February 20, with a freight train outside Syracuse, NY. **The two trains came so close to smashing head−on that the crew of the CSX freight train slammed on the breaks and jumped from the locomotive while it was still moving. "We are taking this incident very seriously. It was truly fortunate that everyone did the right thing and no one was hurt," Marcie Golgoski, an Amtrak spokesperson, said Monday.** Investigators will interview both crews, as well as inspect the operating and computer systems of both trains, she said. The incident occurred in the Onondaga County town of Manlius, about five miles east of Syracuse. The more than 100 passengers on the Amtrak train were made to remain in the cars for four hours. Passengers said they were never told what caused the delay.
Source: http://www.newsday.com/news/local/wire/ny−bc−ny−brf−−amtrak− nearco0223feb23,0,273813.story?coll=ny−ap−regional−wire

12.

February 22, Associated Press — **White House letter with ricin released. A letter containing ricin sent last year to the White House threatened to turn Washington into a "ghost town" if new trucking safety regulations went into effect, according to a copy of the letter released Monday, February 23, by the FBI.** The letter, one of two intercepted last year that were signed "Fallen Angel," bore an October 17 postmark from Chattanooga, TN. The White House letter was typewritten on what appears to be yellow legal paper. Although it was addressed to the White House, the letter begins with "department of transportation" and then says: "If you change the hours of service on January 4, 2004, I will turn D.C. into a ghost town. The powder on the letter is RICIN. Have a nice day. Fallen Angel." A similar ricin−laced letter was found October 15 at a mail processing facility in Greenville, SC. In both cases, the author complained about new regulations that mandate more periods of rest for long−haul truckers. Many truckers and companies have raised concerns about lost pay and productivity because of stricter rest requirements. The South Carolina letter also claimed that the author was the owner of a tanker fleet compnay and had access to large amounts of pulp from castor plants, which are the source of the poison ricin.
Source: http://www.daytondailynews.com/news/content/news/ap/ap_story.html/Washington/AP.V6502.AP−Ricin−Investiga.html

[Return to top]

Postal and Shipping Sector

13. *February 23, Federal Computer Week* — **USPS ties incentives to cost cutting. A salary plan that links pay to job performance may not be enough to turn around an organization such as the U.S. Postal Service (USPS), which is struggling financially. But USPS officials say they are determined to reinvigorate the organization's managers by giving raises to only those who help the service meet service standards and cost−cutting goals.** Last October, all 75,000 postal management employees began working under the new incentive plan. Postal officials say they won't know its effectiveness immediately. Raises for information technology managers depend on how quickly they meet deadlines for replacing old computers and networks with new equipment. IT managers also earn incentive pay based on how many percentage points they can trim by eliminating nonessential IT spending.
Source: http://www.fcw.com/fcw/articles/2004/0223/mgt−postal−02−23−0 4.asp

14. *February 23, Washington Post* — **Truckers' work records inspected in ricin search. A federal grand jury has subpoenaed work records for nine truck drivers employed by a Little Rock company that transports mail for the U.S. Postal Service, part of an effort to determine who might have delivered the first ricin−packed letter last year to a South Carolina postal processing center.** Officials of Mail Contractors of America Inc. say that a subpoena received in late November sought driver logs and time sheets, cell phone and telephone records, delivery receipts and expenses. Eight of the truckers make deliveries to the facility near the Greenville−Spartanburg International Airport where a vial of the toxin was discovered last October; and the other driver is a former employee, said Amy Bunch, a spokesperson for the firm. The Mail Contractors' subpoena comes as investigators sort through the drivers involved in trucker relay systems that are used to transport mail across the country. A rig packed with cartons of third−class mail might be handed off to several different drivers before it reaches its final destination.

Source: http://www.washingtonpost.com/wp−dyn/articles/A62842−2004Feb 22.html

[Return to top]

Agriculture Sector

15. *February 23, Reuters* — **USDA says serious form of bird flu found in Texas.** The U.S. Department of Agriculture (USDA) said on Monday that a highly pathogenic strain of bird flu was found in a Texas poultry flock, a more serious type of the virus than that found in three other U.S. states. Bobby Accord, the administrator of USDA's Animal and Plant Health Inspection Service, told a meeting of state agriculture officials that a "high pathogenic avian influenza was found in a flock in Texas." **Accord also said that the USDA has asked Texas to halt exports of any poultry products from the infected area.** He said the USDA received confirmation of the disease earlier in the day from a government animal health laboratory. **It is the first case of highly pathogenic bird flu found in the United States since the mid−1980s.**
Source: http://www.agriculture.com/worldwide/IDS/2004−02−23T155447Z_01_N23473076_RTRIDST_0_BIRDFLU−USA−UPDATE−1.html

16. *February 23, Agricultural Research Service* — **Researchers test system to track cotton products.** The Agricultural Research Service (ARS) and a California−based corporation will work together to develop a tagging system that will be used to trace U.S. cotton and textile components through rigorous manufacturing processes. **The tagging system would involve embedding into cotton fibers hidden information that would allow officials using hand−held devices to authenticate a cotton textile's U.S. source.** "Creating a security tag that costs less than one cent per pound of cotton is important to the U.S. cotton and textile industries and to Customs agents," said ARS Acting Administrator Edward B. Knipling.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

17. *February 23, Associated Press* — **Japan confirms mad cow case. Japanese authorities on Sunday confirmed the nation's 10th case of mad cow disease since the first sick animal was discovered in September 2001.** The Health Ministry made the announcement a day after saying it suspected the nearly eight−year−old Holstein had the brain−wasting illness. The dairy cow tested positive for the disease at a slaughterhouse outside Tokyo on Friday and again in a follow−up screening at a national laboratory on Saturday. Sixty other dairy cows at the sick Holstein's farm were quarantined. Under a comprehensive screening system put in place after the outbreak three years ago, Japan tests every animal that is killed before it enters the food supply. **Authorities said they hadn't determined the cause of the latest case. But the sick animal, born before the ban on meat−and−bone meal in animal feed, was the second to turn up in Kawagawa prefecture, west of Tokyo.**
Source: http://www.contracostatimes.com/mld/cctimes/news/8019033.htm

[Return to top]

Food Sector

18.

February 23, Food Production Daily — **Canadian poultry ban. Following the announcement at the end of last week that a case of bird flu had been discovered on a Canadian poultry farm, international authorities have responded by banning all imports of poultry and related products from Canada.** The move follows tight regulations announced last week in the European Union, China, Brazil, and a host of other nations to control the spread of the disease there. Most nations trading in poultry from Canada have expressed their intention to ban all products from there.
Source: http://www.foodproductiondaily.com/news/news−NG.asp?id=50103

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

19. *February 23, About Agriculture* — **Five Canadian farm workers infected by virus.** Canadian public health officials aren't saying they are worried over five poultry farm workers who have been diagnosed with the flu, and fall short of confirming the human flu is the same H7 strain detected in chickens on a British Columbia farm on Friday. But there is concern the two illnesses are one and the same. **Five of the nine poultry farm workers exposed to chickens with bird flu on the British Columbian farm have developed symptoms compatible with the H7 strain of a virus that's infected the flock, according to Canadian health officials.** But so far, there is no laboratory confirmation that any of the symptoms reported are definitely linked to the infected chickens. British Columbia agriculture officials report about 16,000 chickens on the farm are in the process of being destroyed and that the farm is under strict quarantine. **Health officials are reporting that the health risk is only confined to individuals directly exposed to the infected birds, and there is no threat to the general public.**
Source: http://agriculture.about.com/cs/poultry1/a/022204.htm

20. *February 23, Reuters* — **Bird flu in Texas prompts human health monitoring. The discovery of a serious strain of bird flu on a Texas chicken farm prompted the U.S. Centers for Disease Control and Prevention (CDC) to say on Monday it would monitor human health in the area for the disease even though it does not normally infect humans.** Officials said the Texas flock was infected with a different strain of bird flu than one that has swept across Asia in recent weeks and been blamed for the deaths of at least 22 people. Federal health officials also sought to play down the risk to human health from the strain found in Texas, known as H5N2. The strain responsible for the deaths in Asia is known as H5N1. "Past experience with H5N2 viruses has indicated there is a low threat to public health," Nancy Cox of the CDC told reporters. **The CDC said it was working with state and local health officials to investigate how many people may have been exposed to the infected chickens.**
Source: http://story.news.yahoo.com/news?tmpl=story&cid=571&ncid=751&e=1&u=/nm/20040223/hl_nm/birdflu_usa_dc

21. *February 23, Reuters* — **Interferon protects against SARS virus in monkeys.** Early treatment with a long−acting form of interferon, called pegylated interferon−alpha, seems to reduce lung damage caused by the virus that produces Severe Acute Respiratory Syndrome (SARS) in macaque. **The results suggest that preventive or early post−exposure treatment with interferon may protect health care workers and others exposed to the virus.** Researchers, at the Erasmus Medical Center in the Netherlands, injected macaques with the SARS virus. Treatment with pegylated interferon begun three days before infection substantially reduced virus levels in the lungs four days after infection. The extent and severity of lung damage was reduced by 80 percent. Although less effective than preventive use, interferon administered at one and three days after exposure still reduced lung damage to some extent, compared with that seen in untreated infected animals. The researchers theorize that the reduced level of protection was probably because therapy was started too close to the peak of viral infection in the lungs, which occurs at two days after exposure in macaques. However, peak SARS virus infection in humans does not occur until about 16 days post−exposure. Therefore, the team theorizes that "the time interval during which effective postexposure treatment with pegylated interferon−alpha can be initiated may be longer in humans than in experimentally infected macaques."
Source: http://story.news.yahoo.com/news?tmpl=story&cid=571&ncid=751&e=2&u=/nm/20040223/hl_nm/interferon_sars_dc

[Return to top]

Government Sector

22. *February 23, MSNBC* — **Homeland Security marks one−year anniversary. The Department of Homeland Security (DHS) has made “measurable, visible progress” toward securing the United States, Secretary Tom Ridge said Monday, marking the agency's one−year anniversary.** However, those gains are balanced with tough tasks ahead. “There’s much to be done,” Ridge said. DHS officially began life, under congressional mandate, one year ago Monday but didn’t open its doors as a separate department until March 1. And simply opening the doors was a tremendous achievement, Ridge said, noting that merging 22 separate agencies encompassing 180,000 people “amounted to a full−scale government divestiture, merger, acquisition and startup, all at once” in what was “undoubtedly the biggest change management challenge of all time.” Just making sure there was a stapler on each desk seemed overwhelming in the early days of the department, Ridge said. Text of Secretary Ridge’s remarks: http://www.dhs.gov/dhspublic/display?content=3204
Source: http://msnbc.msn.com/id/4353530/

[Return to top]

Emergency Services Sector

23. *February 23, Federal Computer Week* — **Oregon city builds P2P network.** The city of Medford, OR, is deploying an IP−based broadband communications network with interoperability for first responders and other government agencies. The city plans to go live

April 2 with the first phase, in which individual users can form a communications network with or without the infrastructure. **Initially it will have 100 users, mostly police, fire and public works employees, but government officials plan to deploy it throughout Jackson County.** "As we identify funding we're going to continue to expand the program until we have truly countywide interoperability," said Ron Norris, the Medford police deputy chief. "The beauty of this system is that it becomes more robust with the more users you have." This technology will help Medford, located in southern Oregon near the California border in a region that lacks interoperability with surrounding jurisdictions and the outlying rural areas. Officials said the initial deployment will cost about $700,000, much of it covered by a $500,000 grant from the Federal Emergency Management Agency.
Source: http://www.fcw.com/geb/articles/2004/0223/web−medford−02−23− 04.asp

24. *February 23, Ravalli Republic (Hamilton, MT)* — **Portable courthouse intrigues officials. A fully functioning, self−contained portable courthouse complete with all the county records, to serve as a back−up in the case of an emergency is what Ravalli County Commissioners saw recently during the biannual Montana Association of Counties (MACO) meeting in Billings, MT.** Engineers in Stillwater County developed the concept three years ago, and now it's just another measure the community 45 miles west of Billings is taking for pretty much any disaster situation its authorities can think of, says Gy Moody, project technician. "It's fully capable of working in case the courthouse exploded or imploded," he said of the 40−foot renovated fifth wheel trailer, owned by the county, that was on display at the MACO conference in Billings, attended by county commissioners from all over the state two weeks ago. And with the possibility of natural disasters that exists anyway, such as flooding or fires, the county directed Moody and others to begin creating concepts that turned the trailer into a central command post on wheels, and a condensed courthouse where all the records are backed up daily.
Source: http://www.ravallinews.com/articles/2004/02/23/news/news05.t xt

[Return to top]

Information and Telecommunications Sector

25. *February 23, Information Week* — **Application security standard edges forward. An application security standard known as Application Vulnerability Description Language (AVDL), which was proposed last year, is moving closer to reality.** AVDL is based on XML and is designed to provide a standard way for application vulnerabilities to be defined and classified so all security applications from different vendors that companies use to secure their apps will understand the same language when it comes to security threats. For example, when a new software vulnerability surfaces, a company's vulnerability scanner could scan systems to spot the new flaw. The scanner then could send information to firewalls and patch−management systems, which those applications could then use to automatically adjust to better protect against any potential attacks, such as a worm or a hacker attack. AVDL 1.0 standard is complete and is expected to receive final standards approval next month. Gartner VP and analyst John Pescatore says that **because of the number of application vulnerabilities that surface each week −− sometimes more than 80 are announced −− standards such as AVDL can help companies reduce the threat they face from the moment a vulnerability is discovered to the time it takes them to respond and patch.**

Source: http://www.informationweek.com/story/showArticle.jhtml?artic leID=18100080

Internet Alert Dashboard

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	3127 (mydoom), 445 (microsoft−ds), 135 (epmap), 80 (www), 6129 (dameware), 1434 (ms−sql−m), 443 (https), 23 (telnet), 4899 (radmin), 137 (netbios−ns) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

26. *February 23, Reuters* — **UN probing possible sales of nuclear designs. The head of the UN nuclear watchdog said Monday that the agency is investigating whether other countries besides Libya got hold of designs for nuclear warheads on the global atomic black market.** "We are still trying to understand the network, to see if other countries have received the technology, the weapons designs," Mohamed ElBaradei told reporters after a meeting with Libya's deputy prime minister. ElBaradei said he and the deputy prime minister in charge of the nuclear program, Matoug M. Matoug, agreed to strive to finish confirming the dismantling of Libya's atomic weapons program by June.
Source: http://story.news.yahoo.com/news?tmpl=story&cid=574&ncid=721 &e=4&u=/nm/20040223/wl_nm/nuclear_libya_dc

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at (703)883−3644
Subscription and Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 703−883−3644 for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call (202)323−3204.

DHS/IAIP Disclaimer